REMARKS

The drawings were objected to because sheets 12, 13 and 14 of the drawings contained expressions and tables. The expressions of sheet 12 have been incorporated into the specification by this amendment. The tables of sheets 13 and 14 were part of the specification as filed. The removal of sheets 12, 13 and 14 has been requested as required by the Examiner.

The specification has been reviewed and amended, where necessary, to correct grammatical and typographical errors and to improve idiomatic English. In addition, on pages 2, 3, 4 and 5, the Expressions 1 through 7 have been inserted, as required by the Examiner. These expressions are found sheet 12 of the drawings as filed and on pages 5, 6, 7 and 8 of the priority document, Japanese Application No. 11/007384, the receipt of which was acknowledged in the Office Action mailed July 31, 2002. No new matter has been added.

Claims 1 to 8 are pending. Each of claims 1 to 8 are amended by this amendment.

The disclosed and claimed invention is directed to a cryptographic apparatus and a computer implemented cryptographic method. The apparatus is shown in Figure 1, the computer implemented method is shown in Figure 34. The operation of the apparatus, and the corresponding operation of the method, is shown in Figures 2 to 33.

N. Koblitz in 1988 (N. Koblitz, "A Family of Jacobians Suitable for Discrete Log Cryptosystems", *Advances in Cryptography – Crypto '88*, Shafi Goldwasser, Ed., pp. 94–99, Springer-Verlag (1988)) introduced the idea to use hyperelliptic curves for cryptographic applications. Some cryptographic systems are realized in computers with limited resources, such as smart cards. ARM (Advanced RISC (Reduced Instruction Set Computer) Machine) processors are typically used for embedded applications such as small network devices, controllers, and mobile phones, especially for secure systems such as on-line banking, pay-TV, network security and so on. The

problem of how to decrease the amount of addition and scalar multiplication on the Jacobians of hyperelliptic curves so that the implementation speed can be improved is very important for a practical use of hyperelliptic curve cryptosystems, particularly computers with limited resources and embedded systems.

Claims 1 to 8 were rejected under 35 U.S.C. §101 as directed to non-statutory subject matter. As the claims are now amended, this rejection is respectfully traversed for the reason that the claimed invention is directed to a field of technology (cryptography) and produces a concrete result (permitting or denying access to a secure environment). The claimed invention provides a practical and simplified implementation for calculating the Jacobians of hyperelliptic curves for use in cryptosystems. As a result, computers with limited resources and embedded systems, in particular, can be used in cryptosystems in a variety of applications.

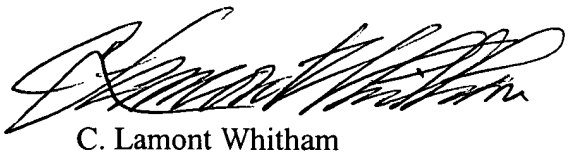
The patent to Orlando et al. (U.S. Patent No. 6,377,969) cited as being of interest but not relied upon has been reviewed; however, Orlando et al. is relevant only in that it relates to the same general field of cryptography. Orlando et al. employ a scalable multiplier architecture which is quite computer intensive and unsuitable to computers with limited resources or embedded systems.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1 to 8 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-0510 (IBM Corporation).

Respectfully submitted,



C. Lamont Whitham
Reg. No. 22,424

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 45773